



PROCUREMENT PACK

Information Security Overview

How Acarise is built, where the data sits, what protects it, and what we have not done yet. Written for the person in your school who has to sign this off.

VERSION	EFFECTIVE FROM
1.0	23 September 2026
AUDIENCE	OWNER
School IT and data protection leads	Acarise Ltd
NEXT REVIEW	CLASSIFICATION
23 September 2027	Public

1. In one page

Question	Answer
Where is the data stored?	Supabase (PostgreSQL), EU region.
Where does the application run?	Vercel.
Is it encrypted?	In transit (TLS) and at rest.
Is it multi-tenant?	Yes, with row-level security enforced at the database.
Do you have SSO?	No. Email and password for staff; email and passphrase for students.
Do you have MFA?	Not yet.
Has it been penetration tested?	Not yet, by an independent tester.
Do you hold Cyber Essentials or ISO 27001?	No.
Does student data train AI models?	No.
Can we get our data out?	Yes — conversations export as text from the product, and a full export on request.

WHY THE "NO" ANSWERS ARE HERE

Acarise is an early-stage product. We would rather a school knew exactly what it is buying than discover a gap after deployment. Where something is missing, it says so.

2. How it is built

Acarise is a web application. There is nothing to install, no agent on a school device, and no inbound connection to a school network. Staff and students reach it over HTTPS from a browser.

Layer	Provider	Region
Application and delivery	Vercel	US
Database and authentication	Supabase (PostgreSQL)	EU
AI models	OpenAI	US
AI request monitoring	Langfuse	EU
Transactional email	Resend	US

The Data Processing Agreement records what each of these receives and the transfer mechanism that covers it.

3. Access control

- **Roles are server-side.** A user's role is derived from server-held account data on every request. Nothing in the browser can change it, and a student account cannot be escalated to a teacher account from the client.
- **Educator accounts are approved individually.** Signing up does not grant access. An Acarise administrator approves each educator before they can create anything.
- **Teacher screens and APIs are closed to students.**
- **Actions on a student are scoped to their teacher.** A password reset, for example, is permitted only to an educator whose group that student belongs to — not to any educator.
- **Row-level security** policies restrict access at the database layer, so an application-layer mistake does not by itself expose another tenant's data.

4. Credentials

- Staff sign in with an email address and a password.
 - Students sign in with an email address and a four-word passphrase, generated by the platform and issued by their teacher. It is shown once and can be reissued.
 - Passwords and passphrases are stored hashed, never in readable form.
 - Acarise never asks a user for their password.
-

5. Assessment integrity

Quiz answer keys are held server-side and are never serialised to the browser. Marking happens on our server. A student cannot read the answers out of the page, the network response or local storage, because they are never sent.

6. AI request handling

- Conversation content is sent to OpenAI to generate each reply. Under the agreement in force, API content is not used to train their models.
 - A copy of each AI request and response is recorded in Langfuse, in the EU, so that faults can be diagnosed and answer quality monitored. **This includes student messages**, and it is called out explicitly in the Privacy Policy.
 - Every AI prompt is versioned, so we can say what the model was asked at any point in time.
-

7. What we do not have yet

This section exists so that nothing on the list above has to be read generously.

Not in place	What that means for you
Independent penetration testing	Our security rests on design and review, not on an external test report. We will commission one.
Cyber Essentials / ISO 27001	No certification to cite in a procurement matrix.
Multi-factor authentication	A compromised staff password is enough to reach that teacher's classes. Use a unique password.
Single sign-on	No Google or Microsoft sign-in. Accounts are managed separately from your directory.
Content moderation or harm detection	Student messages are not scanned and nothing is flagged. See the Safeguarding Policy — this is the most important gap in the product, not just in this document.
Configurable data residency	You cannot choose a region. The split is as set out above.

8. If something goes wrong

Report it to contact@acarise.com. For a personal data breach affecting your pupils we notify you without undue delay and within 48 hours of becoming aware, with the detail the Data Processing Agreement requires, so that you can meet your own obligation to the ICO.

If you believe you have found a security vulnerability, please tell us before telling anyone else, and we will work with you on a timeline for disclosure.

9. Getting your data out

- A teacher can export any student's full conversation as a text file from the product, at any time.
- A school can request a full export of its data, which we provide in a machine-readable format.
- On termination we delete or return the data at your choice; the default is deletion 12 months after termination, and you can ask for it sooner.
- Archiving an activity hides it from students but does not delete it. There is no delete function in the product — ask us if you need material removed.

VERSION HISTORY

Version	Date	Change
1.0	23 September 2026	First issue.

OWNER

Acarise Ltd

CONTACT

contact@acarise.com

NEXT REVIEW

23 September 2027

Acarise Ltd · 283 Uxbridge Road, London W12 9DT · Company No. 16831261, registered in England and Wales · contact@acarise.com